Liability of internet intermediaries

Schellekens, M.H.M.

Published in:
SCRIPTed

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

scripted

Volume 8, Issue 2, August 2011

LIABILITY OF INTERNET INTERMEDIARIES: A SLIPPERY SLOPE?

Maurice Schellekens [*]

Abstract

Should Internet intermediaries do more to prevent illegal and harmful content than they do now? A negative answer to this question is sometimes underpinned by a slippery slope argument. This posits that an intermediary cannot begin doing more, for once he gives in to demands for new duties of care, the range of demands will quickly increase and it may be hard to identify a plausible cut-off point where the intermediary can begin to refuse accepting further duties of care. So, according to the argument, the intermediary is better off not accepting duties of care at all. But is this slippery slope argument valid in the context of liability of Internet intermediaries? Is it really applicable? Is there evidence that a slide would occur? This article examines one such duty of care, viz. a monitoring duty, asks how this duty of care could fit in the relevant European regulation of e-commerce and analyses whether a slippery slope argument for fending off monitoring duties has merit. In doing so, a framework for testing slippery slope arguments is distinguished and applied to the case of monitoring duties. Case law from a number of European countries is analysed to shed light on the likelihood that well-known slippery slope mechanisms can work in the context of Internet intermediary liability.

DOI: 10.2966/scrip.080211.154

[*] Lecturer, Tilburg Institute for Law, Technology, and Society.

1. Introduction

Internet intermediaries, such as Internet Service Providers (hereafter ISPs) or online marketplaces are, under certain conditions, liable for the content that their subscribers or even other Internet-users put online. In Europe, the prevalent model of ISP-liability for third party content is knowledge-based.[1] Apart from the duty to remove expeditiously illegal content that they know of, there are few duties of care resting on hosting intermediaries. This status quo is however not uncontested. Sometimes an argument is made for extra duties of care, such as an obligation to verify the identity of new subscribers, an obligation to suspend Internet access of repeat offenders[2] or the obligation to proactively monitor for certain illegal content. A recent example of the latter is the *SABAM v Tiscali* case: SABAM – the Belgian collecting society for authors of musical works – pressed the ISP Tiscali to engage in monitoring the works of the authors it represented. The case was brought before the court of first instance in Brussels.[3] Having heard an expert on the feasibility of monitoring, the court decided that Tiscali should engage in proactive monitoring. Tiscali appealed against the decision. At the time this article was written, the appeals court has asked preliminary questions to the European Court of Justice in Luxemburg about the interpretation of a number of relevant directives, such as the *Directive on e-Commerce*.[4] This article will focus on monitoring duties and it will leave the subject of other duties of care aside. One of the arguments against imposing monitoring duties on Internet intermediaries is the slippery slope argument. Once an Internet intermediary is subjected to a first monitoring duty its monitoring duties would, according to the argument, quickly snowball. If we – for the sake of argument – assume that those seeking to prevent distribution of pictures of child abuse might be the first to establish a monitoring duty, then others, like victims of libel and slander, of fraud, etc., would soon press for monitoring duties too. The music authors, the film industry, the photographers, the publishers, the holders of trademarks, and the holders of database rights would quickly follow and there would be many more. Eventually, the intermediary would become a gatekeeper to the Internet required to decide about the legality of content, even if nobody complained or where only the slightest or most improbable objections

---

[1] See e.g. art. 14 of *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (*hereafter *Directive on e-Commerce)* (2000), available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32000L0031&model=guichett (accessed 28 July 2011).

[2] See e.g. the British *Digital Economy Act 2010*; B Farrand, "The Digital Economy Act 2010 – A Cause for Celebration, or a Cause for Concern?" (2010) 32 *European Intellectual Property Review* 536-541; N Eziefula, "Getting in on the Act: Ofcom Publishes Draft Code on Digital Economy Act Initial Obligations" (2010) 21 *Entertainment Law Review* 253-256.

[3] For an unofficial translation into English see J Hughes, F Mady and J Bourrouilhou, "English Translation of *Sabam v S.A. Tiscali* (Scarlet), District Court of Brussels, 29 June 2007" (2007), available at http://ssrn.com/abstract=1027954 (accessed 28 July 2011).

[4] Court of Appeals Brussels, 28 January 2010, 2007/AR/2424 and Reference for a preliminary ruling from the Cour d'Appel de Bruxelles (Belgium) lodged on 5 February 2010: *Scarlet Extended SA v Société Belge des Auteurs, Compositeurs et Éditeurs (SABAM)*, Case C-70/10, [2010] OJ 2010/C 113/30.

existed against the content. Under the threat of liability, the intermediary could be nudged into an elaborate form of private censorship. The main thrust of the slippery slope argument is that a possible undesirable outcome (e.g. private censorship) is a reason for the intermediary not to engage in monitoring at all, i.e. not make a first step on the slope. Once a step has been placed on the slope, users of the slippery slope argument contend, an inevitable slide to the bottom will occur. Although the slippery slope is often mentioned as an argument against monitoring it has never been elaborated in the context of ISP liability.[5] This article seeks to fill that void. The central problem addressed in this article can therefore be formulated as follows: what merit is there in advancing a slippery slope argument in order to fend off monitoring duties for ISPs?

This article is constructed as follows. In the following section, a number of basic definitions and terms, and the approach taken towards slippery slope arguments, are explained. In the subsequent section, different types of slippery slope arguments are outlined with their potential application to monitoring by ISPs. The third section evaluates the slippery slope argument as applied to the problem of ISP monitoring duties. Finally, a number of concluding insights are presented based on the foregoing analysis.

2. Preliminary Issues

2.1. Slippery Slope Arguments in General

A slippery slope is a hidden tactic for working towards an outcome that some others consider undesirable. After starting from a plausible starting point, the tactic proceeds in small steps. Each step follows causally or logically from the preceding step. The result is presented as a *fait accompli* being the "natural" result of causal steps taken, or it is given a sense of plausibility as the result of logical steps beginning at a plausible starting point. However, outside the context of the step-trail, the result need not be natural, unavoidable or plausible at all. In fact, some might find it highly undesirable. A slippery slope argument is the converse use of a slippery slope tactic. An opponent of the result will claim that the steps are not mere isolated events, noting that together they form a step-trail that leads towards a specific result and arguing that this result should be judged on its own merits and not "justified" by the implicit normativity of the step-trail. Their argument is thus that no initial step must be made because that would be the start of a slippery slope towards a result that they deem undesirable. The underlying assumption is that the implicit normativity is a very strong mechanism. A slippery slope argument can therefore be fallible. The assertion that once a step upon the slope is placed, an unavoidable slide to the bottom of the slope will occur is not necessarily true. For a slippery slope argument to hold, many statements about future facts and developments must also hold true, or perhaps better, be highly probable. Furthermore, users of slippery slope arguments often use them as

---

[5] P Hunter, "BT's Bold Pioneering Child Porn Block Wins Plaudits Amid Internet Censorship Concerns" (2004) *Computer Fraud & Security* 4-5; E Ackerman, "Censorship Down Under: Australia's proposed Internet restrictions would be more sweeping than any yet seen in a democratic country" (2010) 47 *IEEE Spectrum* 8-9. Critical of the slippery slope argument: A E White, *Virtually Obscene: The Case for an Uncensored Internet* (Jefferson, NC: McFarland & Company, 2006) at ch 3, s 5, "The Negative Argument: A Slippery Slope".

rhetorical instruments and may thus not be as conscientious as might be desirable, in a properly conducted debate, in underpinning the putative steps "down the slope" with evidence. Such approaches have resulted in slippery slope arguments gaining a reputation as exercises in sophistry.[6] However, slippery slope arguments need not be considered as misleading or unhelpful by default. Slippery slope arguments can fulfil useful roles in debates. If a first step could set a sequence of events or decisions in motion that is likely to lead to a bad result, then a slippery slope argument may provide a useful warning that a rational person would take into account when rendering a decision. Slippery slopes may be more or less convincing or valuable as predictors of future results, depending on the probability that further steps down the slope actually will occur. A slippery slope argument may be rightly regarded as a fallacy if, through rhetorical tricks, a serious discussion about its constituent elements is blocked. But where a serious discussion about these elements takes place and false or invalid inferences are avoided, a slippery slope argument can merely be less convincing and not a fallacy.[7] In section 3 below, there will be discussion of how one might test a slippery slope argument in order to be able to say something about its capacity to convince.

2.2. Liability of ISPs in the EU

The liability of providers of information society services in the EU has been harmonised by the *Directive on e-Commerce* of 2000.[8] The Directive introduces absolute and qualified exemptions from liability. For the so-called mere conduit provider the exemption is absolute.[9] An Internet access-provider is an example of a mere conduit-provider.[10] Hosting providers are not liable absent actual knowledge of illegal content. When they receive notice of the presence of illegal content or otherwise gain actual knowledge they need to act expeditiously to remove the content in question or make it inaccessible, or risk losing their exemption from liability. If a hosting provider refuses to act upon knowledge or if he tarries in taking a decision, it can no longer appeal to the exemption and its behaviour will be judged according to the non-harmonised national rules of liability of a Member State.[11] Art 15 of the

---

[6] For a discussion, see D Walton, *Slippery Slope Arguments* (Oxford: Clarendon Press, 1997) , at ch 1.

[7] *Ibid*, 31-36.

[8] For a critical analysis see M Peguera, "The DMCA Safe Harbors and their European Counterparts: a Comparative Analysis of some Common Problems" (2006) 32 *Columbia Journal of Law and the Arts* 481-512.

[9] *Directive on e-Commerce*, see note 1 above, at art 12. For an early court decision leaving the access-provider free to take measures it deems necessary and useful, see *Tribunal de Grande Instance de Paris Ordonnance de Référé du 30 Octobre 2001, Association "J'accuse!...Action Internationale pour la Justice" (AIPJ), La Licra, et Autres c v Association Française d'Accès et de Services Internet (AFA), 13 Fournisseurs d'Accès et Prestataires Techniques d'Internet* (2001), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=205 (accessed 28 July 2011).

[10] Order of the Court (Eighth Chamber) of 19 February 2009 (reference for a preliminary ruling from the Oberster Gerichtshof (Austria)): *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH*, Case C-557/07, [2009] C 113/28.

[11] See e.g. *Cour d'Appel de Paris 14ème Chambre, Section A Arrêt du 12 Décembre 2007, Google Inc v Benetton, Bencom*, available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2116 and *Tribunal de grande instance de Paris Ordonnance de Référé 29 Mai*

directive declares that no *general* duty to monitor may be imposed on providers of information society services, of which an ISP is an example. As a corollary to art 15, Rec. 47 of the Directive states that a *specific* duty to monitor can be imposed on a service provider. Monitoring can be described as checking the legality or illegality of content while there is no specific reason to assume that the content is illegal. Obviously, if monitoring leads to knowledge of illegality, a hosting provider must act expeditiously to remove the content or make it inaccessible. If he does not he loses the exemption from liability the Directive provides and may be found liable under national law. The combination of monitoring and removing the illegal content found will be described here as "filtering". The term "filtering" is not used in the Directive. In sum, the Directive does not create a monitoring duty. It merely leaves the door open for national specific monitoring duties and actually forbids the creation of a general duty. How "specific" and "general" might be demarcated is not specified. Finally, the Directive states that the aforementioned rules do not stand in the way of injunctions against service providers. For copyright infringements, a positive obligation for Member States to have the possibility of injunctions is laid down in art 8.3 *Directive on Copyright in the Information Society* (hereafter *InfoSoc Directive*), which reads as follows:[12] Member States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right. The Enforcement Directive adds that Member States shall also ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to art 8.3 of the *InfoSoc Directive*.[13]

3. The Constituent Elements of the Slippery Slope

A slippery slope has a number of constituent elements. Those elements are a first step on a slope, a result and some driver that explains the progress towards the result. In order to assess the viability of a slippery slope argument in the context of monitoring by Internet intermediaries, the elements of the monitoring slippery slope will be elaborated upon below by describing the arguments the opponent of more monitoring duties for intermediaries actually makes.

2007, Benetton, Bencom v Google Inc, Google France (2007), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2120 (accessed 28 July 2011).

[12] *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society* (2001), available at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32001L0029&model=guichett (accessed 28 July 2011).

[13] *Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights* (2004), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R(01):EN:HTML (accessed 28 July 2011). See also *Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, SEC* (2010) 1589 final, 22-12-2010, COM(2010) 779 final, 7.

3.1. What is the First Step?

A first step in monitoring would be a monitoring duty that is not burdensome and lies in close proximity to the existing behaviour of the intermediary. For example, if an ISP takes certain information off-line following a notification it might monitor whether the content provider places the information online again. Another possibility might be removal of blatant cases of illegality by an ISP, where its attention has been triggered by the amount of traffic the content has created, as illegal content often generates unusual levels of traffic.

As the *Directive on e-Commerce* forbids general monitoring duties, it is worth investigating whether monitoring duties are compatible with the legal framework. The Directive does leave room for the creation of specific monitoring duties. For example, possible monitoring duties that may be compatible with the directive are:

- An intermediary voluntarily monitors for certain illegal content.
- An intermediary falls outside the scope of application of the Directive because it does not act as a service provider "as such". For example, a service provider that also acts as an editor on a forum cannot avail itself of the exemption.
- A service provider must remove clearly illegal content once it obtains knowledge. However, removal of content may be ineffective if a user can simply place the content online again. There is thus an argument that a provider could, or should, perform certain checks to prevent the content from returning.
- The Directive allows for injunctions against service providers. An injunction against the provider may contain a condition requiring monitoring, in one form or another, to prevent the illegal content from returning.

3.1.1. Voluntary Monitoring

An intermediary can monitor content voluntarily. It may do so to provide a service to its subscribers or as a consequence of gentle persuasion by the government. An example is the use of Cleanfeed, a filtering programme originally used by BT and later on, after some pressure from the British government, by other British providers. Monitoring activities started on a voluntary basis may not remain free from commitments. An ISP which incorporates some form of monitoring duty in its subscription agreement, e.g. "We will monitor content to ensure a safe family-friendly environment," may find that failure to do so breaches contractual obligations to its subscribers, or breaches consumer protection laws. Thus, if it advertises its monitoring activities it raises certain expectations with the public that may translate into legal obligations. Nevertheless, for the purpose of this article these activities will be considered to be to be voluntary monitoring, as they are not formally imposed by government. Voluntary monitoring is in accordance with the *Directive on e-Commerce*, as the Directive is concerned with duties that a government imposes upon service providers.

3.1.2. The Intermediary in the Role of Editor

The standard of knowledge applicable to hosting service providers in the Directive is actual knowledge of illegal activity or information and, as regards claims for

damages, awareness of facts or circumstances from which the illegal activity or information is apparent.[14] In many countries the standard to which editors or publishers are held is much stricter. Such stricter liability regime may spur the editor or publisher to take preventive measures, such as proactive checks on the content for which he is responsible. Although at first sight, the role of a service provider and those of an editor or a publisher seem to be easily distinguishable, reality has proven more complex and intricate. The classic example is the American case of *Stratton Oakmont v Prodigy*: Prodigy presented itself as a provider that upheld family values, creating a safe Internet for kids.[15] Prodigy had created content guidelines for its users, had Board Leaders check compliance with those rules and employed screening software to filter out offensive speech. The US Supreme Court decided that Prodigy exercised editorial control and found it liable. It is clear that also in Europe, a provider exercising editorial control, can no longer benefit from the exemptions in the *Directive on e-Commerce*; it assumes the responsibilities that go with the editor-role.[16] However, not all active involvements of an ISP, over and above simply awaiting notices from complainants, will place it in the editor category. If a provider proactively checks for legality without adding any editorial choices of its own, it does not lose his status as a hosting provider.[17] However, it is not completely clear where the division between the provider as a mere technical supporter and the provider in an editorial role lies.[18] Categorising abstracts obtained through an RSS-feed and showing

---

[14] *Directive on e-Commerce*, see note 1 above, at art 14.

[15] *Stratton Oakmont, Inc. v Prodigy Services Co*., [1995] WL 323710 (NY Sup Ct 1995).

[16] See e.g. *Tribunal de Grande Instance de Nanterre Ordonnance de Référé 28 Février 2008, Olivier D. v Aadsoft Com* (2008), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2260 (accessed 28 July 2011); *Tribunal de Grande Instance de Nanterre Ordonnance de Référé 28 Février 2008, Olivier D. v Eric D.* (2008), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2225 (accessed 28 July 2011) and *Tribunal de Grande Instance de Paris Ordonnance de Référé 26 Mars 2008, Olivier M. v Bloobox Net*, (2008), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2256 (accessed 28 July 2011).

[17] See e.g. *Tribunal de Grande Instance de Paris 3ème Chambre, 3ème Section Jugement du 24 Juin 2009, Jean-Yves Lafesse et Autres v Google et Autres* (2009), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2682 (accessed 28 July 2011). Especially the following sentence:

> Si la société Google Inc est amenée à supprimer "ab initio" des contenus c'est en raison de contraintes légales et non par choix personnel; de même c'est pour essayer de lutter contre les contenus illicites qu'elle est amenée à mettre en place des outils de prévention, politique qui ne saurait lui faire perdre sa qualité d'hébergeur.

See also *Cour d'Appel de Paris 14ème Chambre, Section B Arrêt du 21 Novembre 2008, Bloobox Net v Olivier M.* (2008), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2488# (accessed 28 July 2011) and *Tribunal de Grande Instance de Paris 3ème Chambre, 2ème Section Jugement du 14 Novembre 2008, Jean-Yves L. et Autres v Youtube et Autres* (2008), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2484 (accessed 28 July 2011).

[18] For a discussion about issues involved, see e.g. *Cour d'Appel de Paris Pôle 5, Chambre 1 Arrêt du 14 Avril 2010, Omar S. et Autres v Dailymotion* (2010), available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2904# (accessed 28 July 2011).

them on a website was not found to constitute editorial activity.[19] However, an intermediary placing commercial advertisements on, or next to, personal pages of subscribers was treated as an editor.[20] In another case, commercial advertising was found to be not enough to qualify a video-site as an editor, although it was found to be liable on other grounds, viz. inducing copyright infringement by not reacting adequately to notifications.[21] The fluidity of the border between the service provider as such, and the role of editor, permits the holding of intermediaries to stricter standards than those mentioned in art 14 of the Directive.

3.1.3. Monitoring Based on the Obligation to Act upon Knowledge

The German Bundesgerichtshof derived a monitoring duty from competition law and statutes protecting minors against harmful content.[22] The court found that the duty was in accordance with the Directive because it followed from the duties that rest upon a hosting provider once it obtains knowledge. The monitoring duty imposed on eBay – i.e. the hosting provider - was quite elaborate. eBay not only had to monitor for resubmission of the same harmful content by the same content provider; it also had to check that others did not offer the same content, and that the content provider in question did not put up for auction content that was similar to the content that was removed.

3.1.4. Monitoring Based on an Injunction

The Directive allows for injunctions against service providers. It does not specify the contents of such injunctions. That may be interpreted as creating room for a monitoring duty in the form of a prohibitory injunction. The case of *Tiscali v SABAM*, mentioned in the introduction, is a good example. The Brussels Appeals Court has asked the ECJ two questions.[23] The first question asks whether the relevant European directives and the European Convention on Human Rights authorise a national court to order an ISP to filter all electronic communications passing through its service, in

---

[19] See *Tribunal de Grande Instance de Nanterre 1ère Chambre Jugement du 25 Juin 2009, Olivier D. v Wikio* (2009), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=2680 (accessed 28 July 2011).

[20] Offering commercial advertisements on personal pages may make a provider an editor: *Cour d'Appel de Paris 4ème Chambre, Section A Arrêt du 7 Juin 2006, Tiscali Media v Dargaud Lombard, Lucky Comics* (2006), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_articles=1638 (accessed 28 July 2011). See also *Tribunal de Grande Instance de Paris 3ème Chambre, 2ème Section Jugement du 13 Juillet 2007, Christian C., Nord Ouest Production v Dailymotion, UGC Images* (2007), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=1977 (accessed 28 July 2011).

[21] See *Tribunal de Grande Instance de Paris 3ème Chambre, 2ème Section Jugement du 13 Juillet 2007, Christian C., Nord Ouest Production v Dailymotion, UGC Images* (2007), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=1977 (accessed 28 July 2011).

[22] BGH, *Urteil v 12.07.2007, Az. I ZR 18/04*, available at http://www.telemedicus.info/urteile/238-I-ZR-1804.html (accessed 28 July 2011).

[23] Reference for a preliminary ruling from the Cour d'Appel de Bruxelles (Belgium) lodged on 5 February 2010: *Scarlet Extended SA v Société Belge des Auteurs, Compositeurs et Éditeurs (SABAM)*, Case C-70/10, [2010] C 113/30. Compare to the Reference for a preliminary ruling from the Rechtbank van eerste aanleg te Brussel (Belgium) lodged on 19 July 2010: *Belgische Vereniging van Auteurs, Componisten en Uitgevers (Sabam) v Netlog NV*, Case C-360/10 [2010].

particular by means of peer to peer software, with the aim of identifying electronic files containing a work to which the claimant alleges to enjoy rights, and to then block the transfer thereof. If the ECJ answers this question affirmatively, the Brussels court wants to know whether the directives require that the national court applies the principle of proportionality when it is asked to rule on the efficacy and dissuasive effect of the requested measure.

One can easily see the step that is taken here: a move from an injunction against an instance of infringement to an injunction based on a work.[24] A right holder does not ask for an injunction against a specific instance of infringement, for example by notifying a webpage that contains an unlicensed work. Instead, the right holder asks for an injunction to protect his works encompassing unspecified present and unknown future infringements and expects the ISP to make sure the works are not transmitted through its servers. The link with specific instances of illegality becomes so weak that in practice a monitoring duty is being requested. Obviously, less far reaching monitoring duties could be imposed. For example, a French court has imposed a duty to prevent certain content from re-appearing during a period of two years.[25] The duty was limited to two years because of the injunction's provisional character.

3.2. What is the Eventual Outcome?

The eventual outcome of a slippery slope would be a situation in which many monitoring duties are imposed upon intermediaries. This is undesirable because it may lead to private censorship and it may be inefficient. Both elements - censorship and inefficiency - will be elaborated below in section 4.2.2.

3.3. Break Down in Different types of Slippery Slope Arguments

There is a distinction between different types of slippery slope arguments. Here, I distinguish the following types of slippery slope arguments: empirical, logical and full slippery slope arguments. The full argument basically is an argument that combines elements from the two previous types of argument. How the arguments function in the context of ISP monitoring will be dealt with below.

Empirical Slippery Slope Arguments

In this type of argument a number of social or psychological events are linked together to form a causal chain that starts with a first step and ends with an outcome that the person making the argument considers undesirable. Volokh has described a

---

[24] The issue is also raised in question 9 (c) of the preliminary questions in the British case *Lóreal v eBay* pending at the ECJ. See Reference for a preliminary ruling from High Court of Justice (England and Wales), Chancery Division, made on 12 August 2009: *L'Oréal SA, Lancôme Parfums et Beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Limited v eBay International AG, eBay Europe SARL, eBay (UK) Limited, Stephan Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi*, Case C-324/09, [2009] OJ C 267/71.

[25] See e.g. *Cour d'Appel de Paris Pôle 1, Chambre 4 Arrêt du 26 Mars 2010, Youtube v Magdane et Autres* (2010), available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2903 (accessed 28 July 2011).

number of mechanisms through which such a chain can come into being.[26] Hereafter, the mechanisms discerned will be explained and applied to the case of the monitoring intermediary.

Cost Lowering Slippery Slope

A first court imposing a monitoring duty forces an intermediary to make a large investment in a filter-infrastructure. Once the infrastructure is in place, a later court may find it easier to impose a second monitoring duty because the initial investment in the infrastructure is by now a sunk cost. Once an infrastructure for monitoring and filtering is in place its use will be increased. Mission creep will set in. The infrastructure will be used for other content types than initially envisaged and for less damaging illegal content.

Multi-peaked Preferences Slippery Slope

Some courts may find that there is a relevant difference between light and full monitoring: a light form of monitoring can be demanded from an intermediary, not so full monitoring. The court may thus favour the creation of a duty to monitor and filter only those cases that are legally obvious, a form of light monitoring. Other courts on the other hand may oppose all monitoring but value equality much more than non-monitoring. The other courts thus find that if an intermediary monitors for some types of illegal content, there is no argument for allowing him not to monitor for other types of illegal content. So if a court from the first category creates a light monitoring duty, a court from the second category may take this further by requiring full monitoring, even though this court was at first opposed to monitoring at all.

Attitude Changing Slippery Slope

Courts do not have endless amounts of time to scientifically or empirically evaluate the effects of monitoring. If an earlier court decided that it is feasible or proper for an intermediary to filter and the time to seek out all the pros and cons of filtering is in short supply, a court may take the earlier courts findings as a heuristic for the feasibility of filtering. So once a decision has been taken that an intermediary should monitor for some kind of illegal content, a court may conclude that monitoring is a good cause, thus opening up the possibility for much wider monitoring duties. Once an intermediary engages in filtering for one kind of illegal content, it may be difficult to uphold in a discussion that filtering for other "crimes" is not possible.

Small Change Tolerance or Frog Boiling

In a situation where an ISP normally only reacts to notices of illegal content a decision bluntly imposing a monitoring duty on an ISP may seem a bold step. But a decision to monitor the behaviour of a subscriber after an injunction telling the ISP to remove content and check whether the subscriber puts the content back on line may feel as a small step that does not immediately raise difficult questions with respect to information freedoms or the economic efficiency of monitoring. Once a type of monitoring is accepted, monitoring duties can expand in small steps that seem

[26] E Volokh, "The Mechanisms of the Slippery Slope" (2003) 116 *Harvard Law Review* 1026-1079. Mechanisms explored in F Schauer, "Slippery Slopes" (1985) 99 *Harvard Law Review* 361-383 are not addressed in this article.

unproblematic because of their proximity to previous steps that have gained wide acceptance.

Political Power Slippery Slopes

If certain intermediaries start monitoring, the subscribers having the most difficulty with that may choose to subscribe to the services of other intermediaries. The remaining subscribers with the monitoring intermediaries are the ones that are indifferent to monitoring or even applaud it. So the monitoring intermediaries will feel less inhibited by their own subscribers to engage in further monitoring.

Political Momentum Slippery Slopes

The first decision imposing a monitoring duty may function as a release mechanism, unleashing the frustration of many complainants at once. If an ISP starts monitoring this will be seen as a major shift: ISPs are finally found to be responsible for the content they host. A climate may come to exist in which it is taken for granted that ISPs monitor for all kinds of wrongs that may rear their head on the Internet. If society shifts to a view in which it is normal that an ISP acts proactively against unlawful content, a court may be tempted to no longer accept that an ISP denies further reaching monitoring duties.

There is also an economic aspect to this. The cost of monitoring falls on the Internet intermediary. Complainants do not bear the cost. For them, the cost of monitoring is an externality. Once a court imposes one monitoring duty, there is no economic reason for complainants to be reticent with demands for more monitoring duties.

The Structure of Logical Slippery Slope Arguments

A logical slippery slope tactic is one where an object O_i has a certain property P, for example monitoring for clear cases of child pornography has the property that it is proportional. By stressing the similarity of the only slightly different object O_{i+1} to O_i another party is made to concede that O_{i+1} also has P. These steps can be repeated and lead in the end to the concession that also O_j has P. However, it is questionable whether O_j does have property P and had the other party been asked out of the blue whether O_j has P he would have denied it. It is only because of the series of gradual concessions that the party is made to concede that O_j has P. Given that the differences between each pair of O_n and O_{n+1} are small enough, it is the demand of consistency that drives the other party to concede that each next object has the property too.

Such a way of reasoning based on small steps and appealing to the demands of consistency may find application in the context of ISP monitoring duties. Once a court finds that a monitoring duty for a serious crime is proportionate, then a stakeholder may argue that monitoring for a slightly less serious crime must then also be proportionate. Being sensitive to the consistency argument, a court may decide in favour of a monitoring duty for this slightly less serious crime as well. By repeated steps of this type courts may in the end create elaborate monitoring duties for many types of illegal content. In other words, it may lead to a situation where elaborate monitoring duties are said to be proportional.

The Driver of Logical Slippery Slope Arguments

In the context of ISP liability, this may look as follows. Not all filtering activities are alike. They may be distinguished on the basis of a number of characteristics, such as: the (monetary) cost of detection, the complexity or ease with which the case can be evaluated legally, the chance that false positives or negatives occur, the societal benefit in removal of the content from the Internet and the value of the content which is forgone if the content is taken off line. Proponents of monitoring duties may try to obtain a first result in an easy case, i.e. a case of illegal content that can be easily detected, that is legally clear-cut, where the societal benefit of the content is low and the societal value of removal of the content is high. Possibly, a blatant case of child abuse content is an example, because it is such a horrendous crime, the chilling effect on information freedoms may be small or at least proportionate in view of the harm done and the economic impact of monitoring for obvious cases of child abuse content seems to be bearable. Although, when viewed on its own, it may be perfectly reasonable to impose such a limited monitoring duty, a court may nonetheless refuse to do so, because one monitoring duty will lead to another etc. and there is no way to non-arbitrarily or authoritatively indicate where monitoring is no longer proportionate.

Full Slippery Slope Arguments

There is no reason why "causal" mechanisms and logical arguments could in practice not be combined and work together to make the slope even more slippery. In fact, the same phenomenon may have both causal and logical aspects. This can easily be seen by asking oneself the question why a slippery slope tactic executed by making small steps is able to proceed? Is that because there is small change tolerance (which is causal) or is it the demand of consistency (which is logical)? These two may be very difficult to disentangle in practice.

4. How to Evaluate the Slippery Slope Argument

In section 3.1. above a framework is presented for evaluation of a slippery slope argument. In the subsequent section it is analysed whether a slippery slope with respect to monitoring duties could exist.

4.1. Framework

To test the slippery slope argument, I will use a framework consisting of the following four elements: [27]

1. Does the first step have merit? If the first step has no merit that in itself is a reason not to make it. The slippery slope argument would no longer be needed to arrive at the conclusion that the first step should not be made. If on the other hand the first step has merit then the reason not to make it must be the slippery slope.

[27] W van der Burg, "Slippery Slope Arguments" (2009), available at http://ssrn.com/abstract=1445308 (accessed 28 July 2011).

2. Is the final outcome bad? This requirement is self-evident. Without a bad outcome at the end of the slope there is no reason to warn against the slippery slope or the first step on the slope.
3. Is it plausible that the first step will lead to a bad final outcome? This is also a self-evident requirement for a slippery slope argument. The existence of a slippery slope can be countered by stating that either the bad outcome will materialise irrespective of the "first step" or by stating that there is a cut-off point well before the final outcome is reached.
4. Is the current situation adequate? If the current situation is adequate, it need not be changed and there is no reason to take the risk of the first step and possibly the risk of the slide down the slope. However, if the current situation has serious drawbacks, the risk calculus may yield another result and a few steps moving away from the current situation may be worth the risk.

4.2. Evaluation

4.2.1. Merits of the First Step

In the context of the liability of Internet intermediaries the questions of the merits of the "first step" basically means: is monitoring easy cases worthwhile? In order to answer that question one needs to know whether it is at all possible to distinguish easy cases from hard ones. Given the masses of content on the Internet and the amount of content with which something is wrong, it is probably possible to find some easy cases of which it is apparent that they are illegal. This may e.g. be the case where copyrighted content is technically protected, the content is offered together with a crack and for free and the context in which this happens is not likely to be a context in which a right holder is likely to offer his work. Clearly illegal content is to some extent recognisable when you see it. However, it is difficult to describe *in abstracto* how hard and easy cases can be distinguished from each other. The border will certainly not coincide with types of illegality. For example one cannot say that child porn cases are by definition always easy cases and libel is always difficult. Each type of illegality will have its own hard and easy cases.

An argument for denying that a distinction between hard and easy cases can be made is that intermediaries can make mistakes even in simple cases. The BoF-experiment could be mentioned as an example. The civil rights organisation Bits of Freedom (hereafter BoF) conducted some years ago an experiment in which it placed public domain information on the Internet at ten different host providers.[28] It concerned writings of a well-known Dutch author who died more than seventy years ago. Hence, the copyright in the work had expired and this can be considered to be a well-known fact in the Netherlands. Pretending to be a lawyer, BoF then requested that those ten providers remove the content because it allegedly infringed a copyright. Seven out of ten providers were quick to remove the texts even though they belonged to the public domain. So even in simple cases intermediaries can get it wrong. Admittedly, the

[28] S Nas, "The Multatuli Project: ISP Notice & Take Down" (2004), available at http://www.bof.nl/docs/researchpaperSANE.pdf (accessed 28 July 2011).

faux-pas were here somewhat stimulated by the misleading writings of the so-called solicitor. Nonetheless, the concerns raised about things going wrong even in easy cases cannot be dismissed as nonsense. However, this would not deny the possibility of monitoring in easy cases altogether. There are other ways to address these concerns. For example, a low threshold procedure to dispute the decision of an ISP could come some way in addressing the concerns.

An additional argument that some monitoring is possible is provided by online marketplaces and auction sites that long since have programmes in place to monitor the contents of offerings.[29] Apparently, the private benefit and risk calculus here is in favour of monitoring. As sometimes is said the characterisation of the first step of a slippery slope is often only possible after much time when things have crystallised further.[30] For the time being however, I would not categorically deny the benefit of filtering in easy cases.

4.2.2. Objections Against the Final Outcome

Private Censorship

A view of the final outcome is that the intermediaries will become gatekeepers of the information available on the Internet. The risk is that they will engage in private censorship, driven by the fear of being held liable if they fail to remove illegal content from their servers. This might still be an acceptable outcome if it meant that they only remove illegal content which is detrimental to society or particular persons or organisations. However there is a distinct risk that also legal content will be blocked. There are a number of reasons why this may happen.

First, for an ISP, removal of content has little consequences, even if it concerns legal content. An ISP's terms and conditions may even stipulate that it may take down material without notice or recompense. However, failure to remove illegal content has clear and direct consequences in the form of liability.[31] Hence, there is no incentive for ISPs to accurately distinguish between legal and illegal content. Private censorship is likely to occur. The BoF-experiment described above provides some anecdotal evidence that this is not just pure theory: providers do seek ways to deal with doubts about the legality of content in a – for the ISP – efficient way. The risk of false positives was incurred without much ado.

Second, given the sheer volume of Internet content, filtering can only be done with automated tools.[32] However, technical filtering tools are legally far from perfect.[33] They yield many false positives and sometimes are over-inclusive. The former relates to content that is removed because it is mistakenly thought to be illegal. The latter

---

[29] E.g. e-Bay's Fraud Engine and the VeRo-Program.

[30] W van der Burg, see note 27 above.

[31] N Elkin Koren, "Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic" (2006) 9 *New York University Journal of Legislation and Public Policy* 15-75, at 30-34.

[32] Lemley thinks it cannot even be done with technical tools: M Lemley, "Rationalizing Internet Safe Harbors" (2007) 6 *Journal on Telecommunications & High Technology Law* 101-119, at 102.

[33] TJ McIntyre and C Scott, "Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility", in R Brownsword and K Yeung, *Regulating Technologies* (Oxford: Hart Publishing, 2008).

relates to "legal" content that has been taken down because the filtering technology is not fine-grained enough. An example is IP-filtering. The only way to block access to certain illegal content may be to block the IP-address of the computer on which the content is hosted. As a consequence of such a blockade, all content hosted on the blocked computer will become inaccessible. This may include perfectly legal content. An example of the latter is the attempt of the German DFN network trying to block access to a website containing an issue of *Radikall* magazine.[34] The website was hosted by the ISP Xs4all in the Netherlands. DFN blocked the IP-address via which the website could be reached. This resulted not only in the website of *Radikall* being inaccessible but also other websites hosted under the same IP-address. Hence, there was much collateral damage in the form of "legal" websites being blocked. A targeted blockade was technically too complicated and expensive. In the end, Xs4all regularly changed its IP-address and circumvented the block. DFN saw that its block had become ineffective and stopped all attempts to block the *Radikall* website. The *Radikall* case is not an exception. Dutch research about filtering of child abuse content has shown that filtering results in "structural overblocking".[35] This happens because the tools are not precise, fine grained and timely enough.

The problem of overblocking could perhaps be overcome by using filtering tools differently. They could perhaps be used to make a first selection of suspect content. A manual check of the suspect material would then yield the definitive decision about blocking. However, this too is not readily possible. Even after a first selection the volume of content that has to be checked will be exceedingly large.[36] Even if the problem with the volume could be overcome, it is questionable whether the ISP's human intervention is enough to determine the legality of content adequately. First, even if the law is precise about defining what content is legal and what is illegal, what is clear to a legal practitioner may not be clear to an ISP or its technical and administrative staff. If the legality of content is unclear to an ISP, it will block, since this is relatively risk-free, as we have seen above. However, blocking legal content is a form of censorship. Second, the law *in abstracto* may be able to classify some content as legal and other content as illegal. But in between lies a gray area in which it is not so easy to indicate what the law holds. Where it is doubtful what the law is legal proceedings are needed, with clear procedural rules, allowing each party to bring forward its arguments and an impartial arbiter deciding the issue authoritatively. An intermediary engaging in large scale filtering will decide about and probably remove much of the content in the gray area, without the issues involved ever being discussed adequately. This is an interference with the status quo that lacks legitimacy. That too, is a form of private censorship.

The Inefficiency of Filtering

The inefficiency of filtering has several strands. First, filtering involves high costs for staff and equipment. These costs will probably be passed on to the Internet-users.

---

[34] R Vesely, "German Academic Net Blocks Dutch Site" (1997) *Wired*, available at http://www.wired.com/politics/law/news/1997/04/3265 (accessed 28 July 2011).

[35] W Stol, H Kaspersen, J Kerstens, E Leukfeldt and A Lodder, "Filteren van kinderporno op het net: Een verkenning van technieken en reguleringen in binnen- en buitenland" (2008), available at http://www.wodc.nl/images/1616_volledige_tekst_tcm44_117157.pdf (accessed 28 July 2011).

[36] M Lemley, "Rationalizing Internet Safe Harbors" (2007) 6 *Journal on Telecommunications & High Technology Law* 101-119, at 102.

Their subscriptions will become more expensive. This will have a dampening effect on the number of Internet subscriptions.[37] In literature, it has been pointed that this particularly pernicious for the Internet.[38] The Internet is subject to positive network effects. With every new subscriber the utility of the Internet for the existing subscribers grows. Hence, if the number of Internet-users decreases as a consequence of the rising cost of Internet subscriptions, this will affect the remaining internet-users as well. The internet derives its value from its wide user-base. Given its high cost, filtering may strike at the heart of the internet. Large scale filtering has a reductive effect on the internet industry and go at the expense of innovation of the internet.[39]

Second, when it comes to filtering, the ISP may not be the least cost avoider. As we have seen above some human involvement in the determination of legality may be unavoidable. But where it comes to legally evaluating content the ISP is not the person who is well suited to do this efficiently. The ISP is an outsider to the conflict between complainant and content provider and lacks much of the context information that could make the legal evaluation of the cases simpler. Gathering this information would be burdensome for the ISP and that makes the ISP a less than ideal law enforcer. Zittrain indicates that the case for blocking by ISPs, and particularly by destination-side ISPs is strong.[40] However, the starting point for Zittrain's argument is that a court or government has legitimately labeled certain specific content as illegal. His argument is therefore about the efficiency of blocking access to content that is known to be illegal. This is different from the efficiency of filtering by an ISP where the task to determine the legality of content wholly or partially rests with the ISP.

Finally, filtering may cost more than it delivers. Applying Judge Learned Hand's formula,[41] filtering becomes inefficient where its cost becomes greater than the harm that could be prevented with filtering activities multiplied by the chance of such harm occurring. If there is a slippery slope that stacks filtering duties, such a situation may arguably arise. Whether there are strong drivers for a slide down the slope is dealt with in the next section.

4.2.3 Does the First Step actually lead to the Outcome?

Here, it is assumed that a relevant first step has taken place. Could this first step lead to a slide? Above a number of mechanisms have been described that act as a propellant. What indications exist that these mechanisms could be at work in the context of internet intermediaries' monitoring duties? On the basis of case law, the different mechanisms will be revisited here.

---

[37] M Schruers, "The History and Economics of ISP Liability for Third Party Content" (2002) 88 *Virginia Law Review* 205-264, at 248-249, 252.

[38] *Ibid*, 250.

[39] D Lichtman and W Landes, "Indirect Liability for Copyright Infringement: An Economic Perspective" (2003) 16 *Harvard Journal of Law & Technology* 395-410 at 404-405.

[40] J Zittrain, "Internet Points of Control" (2003) 44 *Boston College Law Review* 653-688. See also R Mann and S Belzley, "The Promise of Internet Intermediary Liability" (2005) 47 *William and Mary Law Review* 239-307, at 278: "Surely eBay is more adept at searching and monitoring its marketplace than Tiffany & Co."

[41] *United States v Carroll Towing Co*., [1947] 159 F.2d 169 (2d Cir.).

Cost Lowering Slippery Slope

There is at least one case in which the cost lowering argument has been used explicitly. In the French case of a Jewish student association against Yahoo, a Paris court had to decide whether Yahoo should filter out auctions featuring Nazi-objects. An important argument of the court for its affirmative answer was that Yahoo undertook already filtering of other objects. According to the court, it would cost Yahoo little to filter for Nazi symbols as well.[42]

Multipeaked Preferences

There are court cases in which strict scrutiny is applied towards the proportionality of the filtering measures that the claimant demands. Filtering is for instance found to be disproportional if it is too coarse grained, i.e. if illegal content can only be blocked together with legal content. This was e.g. a decision of the appeals court of Frankfurt am Main where the blocking of Google's search engine had been requested.[43] Filtering can also be disproportional if it entails a risk of false positives, i.e. legal content is filtered out because its legality has been assessed incorrectly. In *Multimania v UEJF*, the Court of Nanterre had to answer the question whether the ISP Multimania should have monitored the websites it hosts. The discussion focused on the effectiveness and proportionality of possible searches for monitoring purposes. The court found in favour of Multimania.[44] Basically, the argument was that simple searches yielded too many false positives and that finding more precise search terms could not be expected from Multimania, because it required expert knowledge.

---

[42] *Tribunal de Grande Instance de Paris Ordonnance de Référé du 20 Novembre 2000, Association "Union des Etudiants Juifs de France", la "Ligue contre le Racisme et l'Antisémitisme", le "MRAP" (Intervenant Volontaire) v Yahoo! Inc. et Yahoo France* (2000), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=205 (accessed 28 July 2011), stating:

> Attendu que selon les informations figurant au rapport des consultants à l'initiative des demanderesses et qui n'ont pas été sérieusement contestées, la société Yahoo refuse d'ores et déjà sur son service d'enchères les ventes d'organes humains, de drogue, d'ouvrages ou d'objets en rapport avec la pédophilie, de cigarettes, ou d'animaux vivants, toutes ventes qu'elle exclut d'office et à juste titre du bénéfice du premier amendement de la constitution américaine garantissant la liberté d'opinion et d'expression ; Attendu qu'il lui en coûterait très certainement fort peu d'étendre ses interdits aux symboles du nazisme et une telle initiative aurait le mérite de satisfaitre à une exigence éthique et morale que partagent toutes les sociétés démocratiques.

See also *Tribunal de Grande Instance de Paris Ordonnance de Référé du 11 Août 2000, Association "Union des Etudiants Juifs de France", la "Ligue contre le Racisme et l'Antisémitisme" v Yahoo! Inc. et Yahoo France*, available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=219 (accessed 28 July 2011)

[43] OLG Frankfurt a.M. 22.01.2008 – Az 6 W 10/08 MIR 2008, Dok. 024, Rz.1

[44] *Tribunal de Grande Instance de Nanterre 1ère Chambre, Section A Jugement du 24 Mai 2000, Union des Etudiants Juifs de France (Uejf) v SA Multimania Production* (2000), available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=223 (accessed 28 July 2011). This decision was confirmed in appeal: *Cour d'Appel de Versailles 12ème Chambre, Section 1 Arrêt du 16 Mai 2002, Association UEJF v SA Multimania Production (Lycos France)* (2002), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=195 (accessed 28 July, 2011) . In the same vein: *Tribunal de Grande Instance de Paris Ordonnance de Référé du 18 Février 2002, SA Télécom City, José Macia et Nicolas Bakar v SA Finance Net* (2002), available at http://legalis.net/spip.php?page=jurisprudence-decision&id_article=200 (accessed 28 July 2011).

Other courts focus on the character of the services provided by the intermediary and find that he falls in the editor type of liability. Above, some examples of court cases in which advertisements could give rise to editor-type liability were given. The existence of these different types of decisions (proportionality versus editor like involvement) can have an accelerating effect on monitoring duties. Once intermediaries are found to be responsible like an editor the proportionality calculus will be made differently. From an intermediary in an editorial role, it can be expected that he expends more resources on fine-tuning filtering measures in order to reduce the number of false positives.

Attitude Changes

At present the attitude towards monitoring duties can be characterised as "no, unless". This is inspired by the *Directive on e-Commerce* that forbids a general monitoring duty in art 15, but sets the door ajar for special monitoring duties in its recitals 47 and 48. The "no, unless" approach is also reflected in case law.[45] Might the openings that the directive offers for the introduction of monitoring duties be exhausted, leading to an attitude change towards "yes, if" then this would have a strong, encouraging effect on the creation of new monitoring duties. The existence of the "no, unless"-attitude is a strong anchor point that keeps us reasonably stationary at present. Under a "yes, if" approach creation of a new anchor point is extremely difficult. In the field of liability of P2P software distributors, the US decision in the Grokster case[46] introduced the inducement theory. Since then infringement on the basis of inducement has been found in a number of cases.[47] It has been followed by at least one court abroad. In the Dutch Mininova decision the software distributor was found liable on the ground that the US Supreme court had pioneered: the distributor had induced copyright infringement by the users of its software.[48] Once a certain type of decision is pioneered – here indirect infringement through inducement – it is likely to have followers.

Small Change Tolerance and the Logical Slippery Slope

I deal with these two types of slippery slope here together because they are closely related. The willingness to create duties that do not diverge too much from what we presently know can be deduced from decisions that allow for monitoring aimed at checking whether content that has been taken off line following a court order does not return. Examples are *Bundesgerichtshof 12.07.2007*[49] and *Cour d'Appel de Paris Pôle 1*, 26 March 2010, both mentioned above.

Political Power and Momentum

Court decisions are not informed by political power constellations. From case law, no indication can be obtained about the presence or absence of these mechanisms. Governmental policies on filtering are of course directly dependent upon political

---

[45] Many court decisions deny monitoring duties, see the notes above.

[46] *MGM Studios, Inc. v Grokster, Ltd.*, [2005] 545 US 913 .

[47] See e.g. *Arista Records LLC v Usenet.com, Inc.*, [2009] 633 F.Supp.2d 124 (SDNY) and *Columbia Pictures Industries, Inc., v Fung*, [2009] No. 06-05578 (CD Cal.).

[48] Rechtbank Utrecht 26-8-2009, LJN: BJ6008, 250077 / HA ZA 08-1124.

[49] See also BGH 11 March 2004 – I ZR 304/01 (Rolex/eBay).

support. For an example of political power at work in the context of filtering, we can turn to Australia. In 2008, the Australian Labour Party came to power. In the Australian Senate the coalition of the Labour Party was dependent upon the sole senator of the Family First party. This political constellation provided fertile ground to set in motion plans aimed at expanding ISP level filtering of Internet content.[50] However, the plans have not yet been realised due to fierce opposition.

Conclusions

The mechanisms of the slippery slope can be recognised in case law about the responsibility of internet intermediaries for third party content. Some mechanisms are more convincing than others. Especially an attitude change to a "yes, if" approach and cost lowering, e.g. through the availability of better filtering software, seem to be particularly strong mechanisms.

4.2.4. The Adequacy of the Current Alternative

Currently, the prevalent way of dealing with illegal content is Notice and Take Down (hereafter NTD). If monitoring compares favourably with NTD then the risk of the slippery slope may be worth taking. At first glance, the prospect for monitoring looks favourable. If filtering software is used, an intermediary is better equipped to deal with the enormous amounts of illegal content present on the internet. However, monitoring may not be able to weed out all illegal content from the Internet. Should monitoring and filtering be preferred over NTD? NTD has the advantage of the notice which has several beneficial functions. In the first place it shows that the stakeholder is prepared to expend some time and effort in law enforcement. He or she had to write the notice and seek out some facts to inform the ISP of the facts underpinning his or her claim adequately. If the illegal content was too *de minimis* he or she would not have bothered. So it provides an indication that law enforcement in this case is thought to be valuable. The selection element of NTD is important. Both filtering and NTD are not able to address all illegal content. Hence, it is important to have an instrument that indicates what illegal content should be dealt with. Secondly, the notice narrows down the legal issue at stake. Legal grounds not mentioned in the notice the ISP will usually not consider. This allows a more focused evaluation of the points that really matter. Thirdly, the notice provides extra information about the illegal content. The notifier will for example indicate why he thinks the content is illegal and adduce facts and circumstances underpinning his viewpoint. Obviously this information need not be correct. But even incorrect information can be valuable, especially if it is recognisable as such. It provides information about what is at stake. Only where information is downright misleading the context information provided in a notice is detrimental. In case of monitoring, the ISP has to do without the information the notice provides. Arguably, the monitoring ISP has other extra information at its disposal, e.g. a black list built into the filtering tool from which can be read that content X is illegal. However, a black list can be composed without knowledge of the situation of the website or other place where the content is found. So the ISP misses the context specific information that a notice would have provided.

---

[50] D Bambauer, "Filtering in Oz: Australia's Foray into Internet Censorship" (2008) *Brooklyn Law School, Legal Studies Paper* No. 125, available at SSRN http://ssrn.com/abstract=1319466 (accessed 28 July 2011).

This may enlarge the risk that the issues before the ISP are not addressed adequately. In the end, it will remain debatable whether NTD will yield better decisions than filtering. But given that both instruments cannot cope with all illegal content that an ISP may be asked to address, NTD has two important advantages. It does not require a start-up investment because it is already being done and it selects which illegal content should be dealt with.

5. Conclusion

The central issue in this article is whether there is merit in advancing a slippery slope argument to fend off monitoring duties for ISPs. Several types of slippery slope arguments were distinguished and it was explained how these arguments could be applied to the question of the desirability of monitoring by an ISP. Subsequently, a scheme for testing the validity of the slippery slope arguments was presented. The scheme addresses four issues and gave rise to the following findings. At present, the support for more involvement of internet intermediaries seems to be on the rise.[51] At the same time, the current way of dealing with third party content – NTD – may perhaps be seen as a proportionate response to current developments. However, if a limited monitoring duty has some benefit as well – and I think it may have – the question arises whether a limited monitoring duty might still fairly be opposed on the ground that it is a first step on a "slippery slope"? This requires two considerations: 1. Is the situation that results from a full slide down slope undesirable? and 2. Could first monitoring duties have a snowballing effect? With respect to the first question, it is clear that there are very strong arguments that a very high level of monitoring is undesirable, both in terms of the censorship it will entail and in terms of its inefficiency. The main issue is of course whether new monitoring duties could cause a snowballing effect. Two issues need to be addressed here. On the one hand, we must not be sliding already. That is not the case. Although there is some filtering at present,[52] it all seems to be rather fragmented and it is not inconsistent with a "no, unless" approach. On the other hand, a cut-off point somewhere along the slope could negate the danger of a slippery slope. Being a negative fact, the absence of a cut-off point is difficult to prove. Analysis according to Volokh's mechanisms shows that all mechanisms can be found in the context of monitoring by Internet intermediaries. Some mechanisms seem to be stronger than others. Especially, an attitude change to a "yes, if" approach could negate the establishment of a cut-off point. It would lead to a situation in which monitoring duties would be applied by default. An exception would require strong arguments and concomitantly have a small chance of success. Also other mechanisms would not be conducive to stabile cut-off points. Once a filtering infrastructure is in place, it will be tempting to use it and not leave the filtering potential unused. Also progression in small steps and analogising new cases to close, old cases may prove to be strong mechanisms for bringing filtering forward and may

---

[51] T Jones, "12 Trends to Watch in 2010" (2010), available at https://www.eff.org/deeplinks/2010/01/trends-2010 (accessed 28 July 2011), especially trend 3, "Global Internet Censorship: The Battle for Legitimacy".

[52] Online auctions like eBay voluntarily monitor and some ISPs monitor for child porn, e.g. through the British Cleanfeed system. Maybe there is too some hidden filtering by ISPs. There is also organised notification (e.g. the Internet Watch Foundation). Now and then, there is an attempt to block access to content hosted abroad, where it cannot be taken down.

complicate the position of those who want to create a cut-off point. These types of argument have already been used in case law. For now, the use of "propelling arguments" has been too fragmented to have a large impact on monitoring duties. The arguments or mechanisms are – so to say - sleeping, but a high profile decision could awaken them and trigger a slippery slope. Hence, there is every reason to be vigilant.